**Are phones listening to us? What they can learn from the sound of your voice**

November 27, 2018 3.16pm GMT

[Ian McLoughlin](https://theconversation.com/profiles/ian-mcloughlin-217755)

Professor of Computing, Head of School (Medway), University of Kent

The vast majority of people in developed countries now carry a smartphone everywhere. And while many of us are already well aware of privacy issues associated with smartphones, like their ability to [track our movements](http://uk.businessinsider.com/google-tracks-movements-ap-princeton-investigation-2018-8?r=US&IR=T) or even [take surreptitious photos](https://www.forbes.com/sites/josephsteinberg/2013/06/04/your-smartphone-can-photograph-you-and-share-the-pictures-without-your-knowledge/#137f156752c4), an increasing number of people are starting to worry that their smartphone is actually [listening to everything they say](https://www.vice.com/en_uk/article/wjbzzy/your-phone-is-listening-and-its-not-paranoia).

There might not be much evidence for this but, it turns out, it isn’t far from the truth. Researchers worldwide have begun developing many types of powerful audio analysis AI algorithms that can extract a lot of information about us from sound alone. While this technology is only just beginning to emerge in the real world, these growing capabilities – coupled with its 24/7 presence – could have serious implications for our personal privacy.

Instead of analysing every word people say, much of the listening AI that has been developed can actually learn a staggering amount of personal information just from the sound of our speech alone. It can determine everything from [who you are](https://theconversation.com/can-voice-recognition-technology-really-identify-a-masked-jihadi-52787) and [where you come from](https://www.dailymail.co.uk/sciencetech/article-3393935/Can-app-guess-accent-English-Dialects-tool-predicts-hometown-based-pronounce-26-different-words.html), [your current location](https://arxiv.org/pdf/1411.3715.pdf), your [gender and age](https://www.sciencedirect.com/science/article/pii/S088523081630136X) and [what language](https://www.nist.gov/sites/default/files/documents/2016/10/06/lre15_evalplan_v23.pdf) you’re speaking – all just from the way your voice sounds when you speak.

***Read more:*** [***Smartphone data tracking is more than creepy – here's why you should be worried***](http://theconversation.com/smartphone-data-tracking-is-more-than-creepy-heres-why-you-should-be-worried-91110)

If that isn’t creepy enough, other audio AI systems can detect [if you’re lying](https://pdfs.semanticscholar.org/fda7/2ce8b95866dd924326b09fca35a4a68ecab7.pdf), analyse your [health](http://www.good-vibrations.nl) and [fitness level](https://www.sciencedirect.com/science/article/abs/pii/S0167639316302692), your current [emotional state](https://vokaturi.com), and whether or not you’re [intoxicated](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3524529/). There are even systems capable of detecting what you’re [eating when you speak with your mouth full](https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0154486), plus a slew of research looking into [diagnosing medical conditions](https://www.scientificamerican.com/article/the-sound-of-your-voice-may-diagnose-disease/) from sound.

AI systems can also accurately [interpret events from sound](http://www.lintech.org/machine_hearing/index.html) by listening to details like car crashes or gunshots, or environments from their [background noise](http://dcase.community/challenge2018/). Other systems can identify a [speakers’ attitude](https://patents.google.com/patent/US8078470) in a conversation, pick up unspoken messages or detect [conflicts between speakers](https://ieeexplore.ieee.org/document/6289065). Another AI system developed last year can predict, just by listening to the tone a couple used when speaking to each other, whether or not they will [stay together](https://theconversation.com/ai-can-predict-whether-your-relationship-will-last-based-on-how-you-speak-to-your-partner-81420). These are all examples of current AI technology developed in research labs worldwide.

All of these technologies – no matter what they’re trying to learn about you – use machine learning. This involves training an algorithm with large amounts of data that has been labelled to indicate what information the data contains. By processing thousands or millions of recordings, the algorithm gradually begins to infer which characteristics of the data – often just tiny fluctuations in the sound – are associated with which labels.

For example, a system used to detect your gender would record speech from your smartphone, and process it to [extract “features”](http://www.mcloughlin.eu/speech/chapter6.html) – a small set of distinct values that compactly represent a bigger speech recording. Typically, features represent amplitude and frequency information in each successive 20 millisecond period of speech. The way that these fluctuate over time will be slightly different for male or female speech.

Machine learning systems will not only look at those features, but also how much, how often, and in which way the features change over time. While the recording happens in the smartphone itself, clips are sent to internet servers which will extract features, compute their statistics, and handle the machine learning part.

Training an algorithm is done using big data. Professor Ian McLoughlin

AI was first created to perform conceptual tasks normally requiring human intelligence. At the moment, most AI systems perform analysis and understanding tasks, which means they provide information for humans to act on, rather than acting automatically.

For example, audio AI systems for road monitoring can alert traffic controllers to the sound of a vehicle crash, and audio-based medical diagnosis AI would alert a doctor about findings of concern. But a human would still have to make a decision based on the information provided to them by the AI.

But new AI technologies are changing. Many AI systems are starting to exceed human capabilities, with some devices even able to act without human intervention. Amazon Echo and Google Home are both examples of AI that has [thinking abilities](https://www.intechopen.com/download/pdf/5862). This kind of AI can respond to commands directly and can also [act on these commands](https://www.researchgate.net/profile/Chung-Horng_Lung/publication/262359882_Smart_Home_Integrating_Internet_of_Things_with_Web_Services_and_Cloud_Computing/links/5bbcfe06a6fdcc9552dcf8b0/Smart-Home-Integrating-Internet-of-Things-with-Web-Services-and-Cloud-Computing.pdf), like when we ask Alexa to turn on the lights or draw our [smart curtains](https://www.smarthomequest.com/best-smart-windows-drapes/).

While most AI systems today are designed to assist people, in the wrong hands, these technologies could look more like the [Thought Police](https://en.wikipedia.org/wiki/Thought_Police) from George Orwell’s *1984*. Audio (and video) surveillance can already detect our actions, but the AI systems we have mentioned are starting to detect what is behind those actions – what we’re thinking, even if we never speak it aloud.

Most tech firms say their devices don’t record us unless we command them to, but there have been examples of Alexa making recordings [by mistake](https://www.theverge.com/2018/5/24/17391898/amazon-alexa-private-conversation-recording-explanation). And researchers have shown that it doesn’t take much to turn your phone into a [permanent microphone](https://www.bbc.co.uk/news/technology-35639549). It may only be a matter of time before advertisers and scammers start to use this technology to understand exactly how we think, and target our private weaknesses.

Organisations like the [World Privacy Forum](https://www.worldprivacyforum.org/), [Fight for the Future](https://www.fightforthefuture.org/) and the [Electronic Frontier Foundation](https://www.eff.org/) are working to ensure people have the right to privacy from digital sensing systems, or have the right to opt out from commercial surveillance. In the meantime, when you next install an app or a game on your smartphone and it asks to access all sensors on your device, just remember what you are potentially signing up to.

These data collectors could learn to understand you as well as your closest friend and probably better, because your phone travels everywhere with you, potentially listening to every sound you make. But while we can trust a true friend with our life, can we say the same for those who are collecting our data today?